(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 707 409**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **93 08506**

(51) Int Cl[6] : G 06 K 19/073

(12) DEMANDE DE CERTIFICAT D'UTILITE A3

(22) **Date de dépôt** : 09.07.93.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande :** 13.01.95 Bulletin 95/02.

(56) **Les certificats d'utilité ne sont pas soumis à la procédure de rapport de recherche.**

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *SOLAIC (société anonyme)* — FR.

(72) **Inventeur(s) :** Thiriet Fabien.

(73) **Titulaire(s) :**

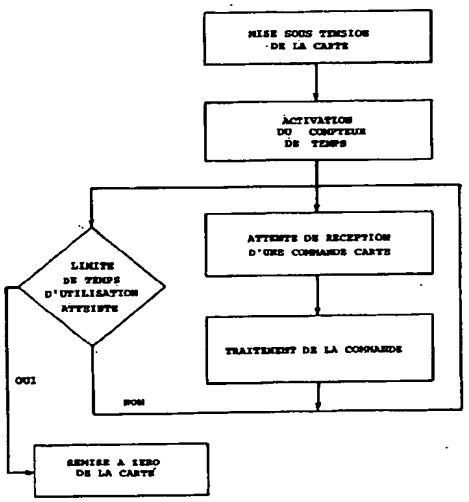
(74) **Mandataire :** Cabinet Malemont.

(54) Procédé pour limiter le temps d'enregistrement ou de lecture d'informations sensibles dans une carte à mémoire, et carte à mémoire pour la mise en œuvre de ce procédé.

(57) Procédé pour limiter le temps d'enregistrement ou de lecture d'informations sensibles dans la mémoire de données non volatile d'une carte à mémoire consistant, lors de l'exécution du programme de la carte et suite à une mise sous tension de celle-ci, à effectuer successivement les opérations suivantes:

- activer un compteur de temps, indiquant le temps écoulé t, ledit compteur de temps étant indépendant du programme de la carte;
- comparer le temps écoulé par rapport à une limite de temps T;
- poursuivre le programme de la carte si t est inférieur à T ou suspendre le programme de la carte si t est supérieur ou égal à T.

Carte à mémoire pour la mise en œuvre de ce procédé.



FR 2 707 409 - A3

Procédé pour limiter le temps d'enregistrement ou de lecture d'informations sensibles dans une carte à mémoire, et carte à mémoire pour la mise en oeuvre de ce procédé.

La présente invention concerne d'une part un procédé pour limiter le temps d'enregistrement ou de lecture d'informations sensibles dans la mémoire de données non volatile d'une carte à mémoire à logique câblée et/ou à microcontrôleur, d'autre part une carte à mémoire pour la mise en oeuvre de ce procédé.

On emploie de plus en plus de cartes à mémoire, qu'elles soient à logique câblée ou à microcontrôleur, pour des utilisations ou des applications très diverses et notamment dans le cas où des informations secrètes, sensibles ou confidentielles doivent être recherchées ou obtenues au moyen d'un ordinateur ou d'un terminal.

Dans les installations connues, les dispositifs de sécurité sont soit inexistants soit très limités. Ils ont pour objet soit d'empêcher la recherche d'informations confidentielles, soit de n'autoriser cette recherche qu'à des utilisateurs dûment accrédités.

On a cherché depuis longtemps à limiter l'accès aux informations sensibles. Pour ce faire, on utilise des mots de passe, le nombre de tentatives pour donner le mot de passe correct étant fixé à un maximum, par exemple un, deux ou trois.

La présente invention se distingue des techniques connues en ce sens qu'elle consiste à incorporer dans une carte à mémoire un système de surveillance du temps écoulé afin de limiter le temps d'enregistrement ou de lecture d'informations dans la mémoire de la carte à mémoire ou du terminal utilisant cette carte.

Pour ce faire, le procédé objet de l'invention se caractérise en ce qu'il consiste, lors de l'exécution du programme de la carte - programme d'exécution des instructions câblées et/ou programme d'exploitation - et suite à une mise sous tension de celle-ci, à effectuer successivement les opérations suivantes :

- activer un compteur de temps, indiquant le temps écoulé t, ledit compteur de temps étant indépendant du programme de la carte ;
- comparer le temps écoulé par rapport à une limite de temps T ;
- poursuivre le programme de la carte si t est inférieur à T ou suspendre le programme de la carte si t est supérieur ou égal à T.

Le procédé permet de limiter la durée d'utilisation de cette carte à une valeur prédéterminée appelée "limite de temps".

Ce procédé implique l'utilisation de cartes à mémoire dans lesquelles il est prévu dans la mémoire de données s'il s'agit d'une carte à logique câblée, ou dans l'une des zones (CPU, ROM, RAM, EPROM, EEPROM) du microcontrôleur s'il s'agit d'une carte à microcontrôleur :

- au moins un compteur de temps, pour compter le temps écoulé t ;
- une zone de données (Z_1, ... T_n) pour stocker des données de limite de temps (T_1,...,T_n), n étant supérieur ou égal à 1 ;
- un comparateur, pour comparer le temps écoulé t aux données de limite de temps limite (T_1, ... T_n).

Selon un mode de réalisation préféré de l'invention, le procédé est mis en oeuvre lors de chaque enregistrement ou lecture de données et, de préférence, pendant une période P de mise sous surveillance de la carte.

Ainsi, le procédé peut non seulement être employé d'une manière générale lorsque l'on utilise la carte à mémoire mais également lors de chaque opération, enregistrement ou lecture de données ; le procédé peut également être employé pendant une période de validité de la carte, que cette période soit temporaire, permanente ou aléatoire, par exemple pendant les dix premiers jours de chaque mois, les jours pairs, etc...

Selon un autre mode de réalisation de l'invention, le procédé selon l'invention est mis en oeuvre pendant une transaction, ou une application, ou l'attente d'une commande

de la carte à mémoire, respectivement, qui doit être achevée à l'expiration de la limite de temps T, faute de quoi la carte est remise à zéro, ou les droits d'accès à l'application sont remis à zéro, ou un message d'erreur est émis, respectivement.

On peut voir ainsi que lorsque la limite de temps est atteinte, les conséquences pour la carte à mémoire peuvent être variées, telle qu'une remise à zéro ou une remise à zéro des droits d'accès à une application donnée ou encore l'émission d'un message d'erreur et/ou d'alerte à destination d'un terminal, d'un ordinateur ou d'un centre de surveillance.

Le procédé selon l'invention peut avantageusement être mis en oeuvre dans une carte à mémoire destinée à gérer un nombre de transactions et/ou d'applications et/ou de commandes 1 à n et, dans ce cas, il est prévu un fichier de temps d'utilisation maximum T_1, ... T_n pour la mise en oeuvre du procédé lors du déroulement de chaque transaction ou application ou de commandes.

Un des avantages essentiels de l'invention est que le principe de limite de temps peut être appliqué au moyen d'un ou plusieurs compteurs de temps, et mis en oeuvre pour surveiller le temps maximum d'utilisation, de transactions, d'applications ou de commandes différentes, chacune d'entre elles ayant son propre paramètre de limite de temps, ce qui rend l'utilisation du procédé extrêmement souple.

On peut également prévoir d'affecter un compteur de temps C_1, ... C_n, par transaction, application ou commande.

L'invention sera décrite ci-après en référence aux trois figures représentant des vues schématiques des différentes étapes du procédé dans les trois cas suivants :

- pour la figure 1, il s'agit du cas général de limitation du temps d'utilisation d'une carte à mémoire qui reçoit une commande envoyée par un terminal ;
- pour la figure 2, il s'agit de la mise en oeuvre du procédé pour une application particulière gérée par la carte

parmi plusieurs applications, par exemple pour la mise à feu d'un missile ; et

- pour la figure 3, il s'agit d'un exemple d'utilisation de carte à mémoire pour la réception d'un protocole de communication normalisé.

Les exemples décrits aux figures 1 à 3 s'appliquent aux différents cas de cartes à mémoire :

- pour une carte à mémoire à logique câblée, elle contiendra au moins une zone mémoire de données non volatile et au moins un compteur de temps ;
- pour une carte à microcontrôleur, elle contiendra d'une part un microcontrôleur (CPU, ROM, RAM, EPROM, EEPROM) et au moins un compteur de temps.

La figure 1 décrit les étapes du procédé dans la cas où un utilisateur emploie une carte à mémoire pour passer un ordre boursier à un terminal ou à un ordinateur de sa banque. Après la mise sous tension de la carte lorsque celle-ci est introduite dans le terminal ou l'ordinateur de la banque, le compteur de temps est activé. Si l'on suppose une limite de temps fixée à dix minutes, le terminal bancaire relié à la carte va comparer à intervalles réguliers, par exemple toutes les secondes, le temps écoulé depuis la mise sous tension de la carte à la valeur limite de dix minutes. Si le temps écoulé reste inférieur à la valeur limite, le terminal pourra rester en attente de réception d'une commande de la carte à mémoire et traiter cette commande, par exemple une remise d'espèces ou autre. Si au contraire le compteur de temps écoulé indique une valeur égale ou supérieure à la limite des dix minutes prévue, la carte à mémoire sera remise à zéro et ne pourra plus être utilisée pour une transaction bancaire. Dans le cas d'une carte à mémoire remise à zéro, le terminal ne peut plus effectuer une quelconque opération qui serait demandée par l'utilisateur.

Ce procédé trouve son application particulière dans le cas où l'utilisateur n'est pas le titulaire officiel de la carte à mémoire mais un fraudeur. Ce dernier se voit donc interdire toute utilisation de la carte, comme par exemple

recherche d'un code secret, lorsqu'il a utilisé la carte plus de dix minutes.

La figure 2 est un exemple d'utilisation d'une carte à mémoire pour la mise à feu d'un missile. Il s'agit du cas où une carte à mémoire contient plusieurs applications, l'une d'entre elles permettant la mise à feu du missile. L'accès à cette application doit être sécurisé de façon à ce que seule la personne habilitée puisse avoir connaissance des paramètres de mise à feu qui sont mémorisés dans un fichier géré par l'application de mise à feu. L'utilisateur pour lire les paramètres de mise à feu doit présenter un code secret qui ouvre un droit d'accès à l'application.

L'utilisation du procédé objet de la présente invention se fait de la manière suivante : la carte à mémoire est placée dans un terminal et mise sous tension ; l'utilisateur choisit l'application de mise à feu, il lui est alors demandé de présenter le ou les codes secrets qui lui permettront d'utiliser l'application et de lire les paramètres de mise à feu du missile. Lorsque les codes secrets sont validés, c'est-à-dire acceptés par la carte à mémoire, les droits d'accès à l'application sont mis à jour et le compteur de temps est activé. Les droits d'accès sont les temps pendant lesquels les codes secrets d'utilisation de l'application sont valides.

Tant que la limite de temps n'est pas atteinte, l'utilisateur pourra lire les paramètres de mise à feu du missile. Lorsque la limite de temps est atteinte ou dépassée, les droits d'accès à l'application sont remis à zéro et il n'est donc plus possible de prendre connaissance des paramètres de mise à feu du missile.

Si l'utilisateur de la carte est la personne normalement habilitée, la mise en oeuvre du procédé est une mesure de sécurité efficace et utile.

Si au contraire l'utilisateur n'est pas la personne habilitée, il pourrait, s'il n'y avait pas de limite de temps, lire dans l'application de mise à feu tous les paramètres de mise à feu du missile et les utiliser.

L'exemple numéro 3 est celui de la transmission au moyen d'une carte à mémoire d'un protocole de communication de données normalisé. L'utilisateur souhaite que soit envoyé à la carte à mémoire une suite d'octets ou de blocs d'informations qui représentent le protocole de communication normalisé. La carte à mémoire, un fois sous tension, est mise en attente d'une commande, appelée "commande carte" et le compteur de temps est activé.

Si la limite de temps, par exemple de dix minutes, de réception de la commande n'est pas atteinte, la carte à mémoire peut recevoir les octets ou les blocs de données de la commande et vérifier que tous les octets ou les blocs de données ont bien été reçus.

Si au contraire le temps d'utilisation de la carte atteint ou dépasse la limite de temps fixée à dix minutes, un message d'erreur est envoyé au terminal qui peut indiquer à l'utilisateur que, pendant la période autorisée, l'ensemble des données du protocole de communication n'a pu être correctement acheminé à la carte à mémoire.

Les exemples ci-dessus sont décrits à titre d'illustrations non limitatives de la présente invention qui trouve son application dans de très nombreux cas d'utilisation de cartes à mémoire lorsque la sécurité impose de limiter le temps d'utilisation à une ou plusieurs valeurs déterminées.

REVENDICATIONS

1. Procédé pour limiter le temps d'enregistrement ou de lecture d'informations sensibles dans la mémoire de données non volatile d'une carte à mémoire à logique câblée et/ou à microcontrôleur, caractérisé en ce qu'il consiste, lors de l'exécution du programme de la carte - programme d'exécution des instructions câblées et/ou programme d'exploitation - et suite à une mise sous tension de celle-ci, à effectuer successivement les opérations suivantes :

- activer un compteur de temps, indiquant le temps écoulé t, ledit compteur de temps étant indépendant du programme de la carte ;
- comparer le temps écoulé par rapport à une limite de temps T ;
- poursuivre le programme de la carte si t est inférieur à T ou suspendre le programme de la carte si t est supérieur ou égal à T.

2. Procédé selon la revendication 1, caractérisé en ce qu'il est mis en oeuvre lors de chaque enregistrement ou lecture de données.

3. Procédé selon l'une des revendications 1 ou 2, caractérisé en ce qu'il est mis en oeuvre pendant une période P de mise sous surveillance de la carte.

4. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il est mis en oeuvre pendant une transaction, ou une application, ou l'attente d'une commande de la carte à mémoire, respectivement, qui doit être achevée à l'expiration de la limite de temps T, faute de quoi la carte est remise à zéro, ou les droits d'accès à l'application sont remis à zéro, ou un message d'erreur est émis, respectivement.

5. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que, pour une carte à mémoire destinée à gérer un nombre de transactions et/ou d'applications et/ou de commandes 1 à n, il est respectivement prévu un fichier de temps d'utilisation

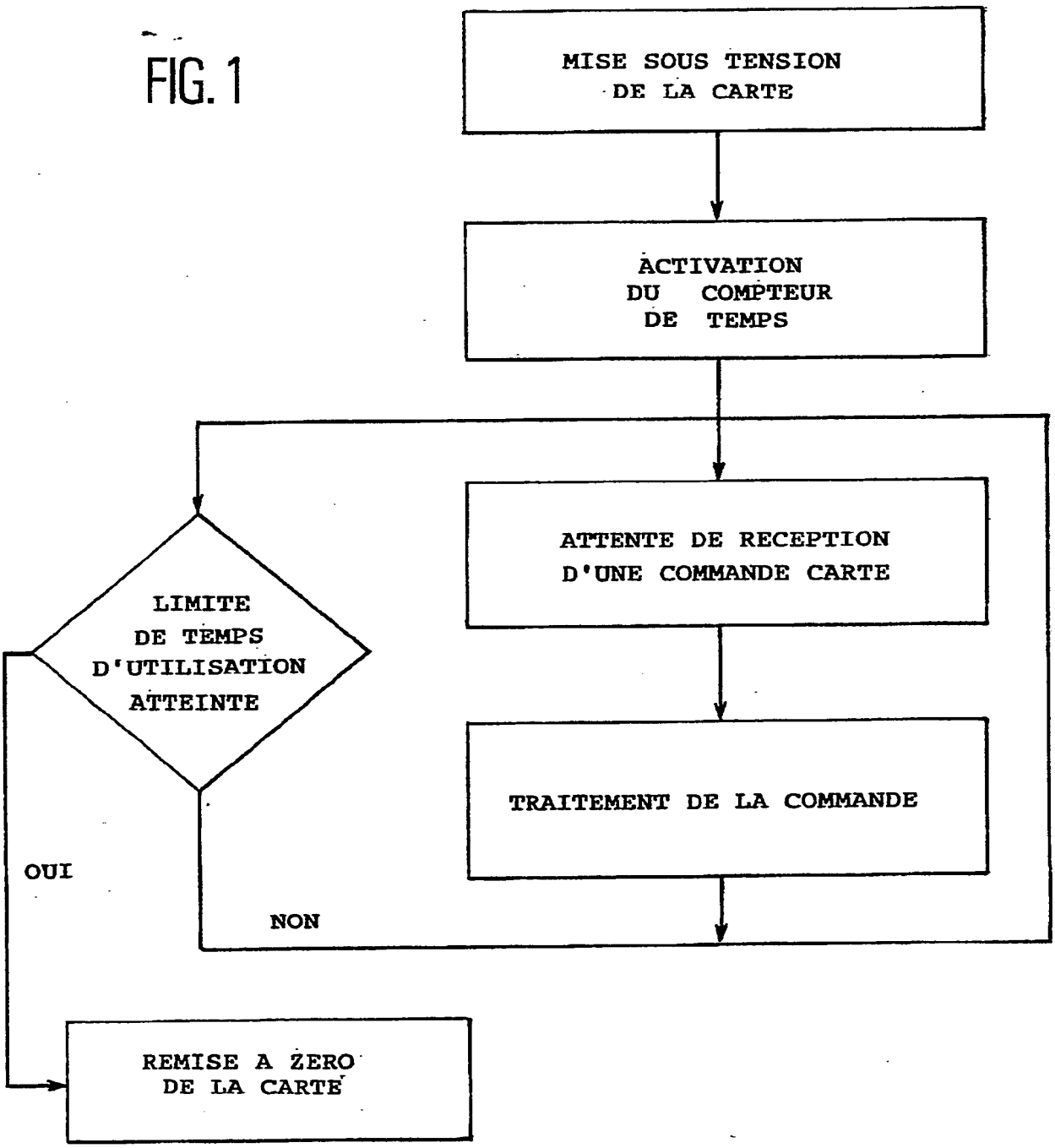
maximum T_1, ... T_n pour la mise en oeuvre du procédé lors du déroulement de chaque transaction (ou application).

6. Carte à mémoire pour la mise en oeuvre du procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il est prévu, dans la mémoire de données s'il s'agit d'une carte à logique câblée, ou dans l'une des zones (CPU, ROM, RAM, EPROM, EEPROM) du microcontrôleur s'il s'agit d'une carte à microcontrôleur :

- au moins un compteur de temps, pour compter le temps écoulé t ;
- une zone de données (Z_1, ... T_n) pour stocker des données de limite de temps (T_1,...,T_n), n étant supérieur ou égal à 1 ;
- un comparateur, pour comparer le temps écoulé t aux données de limite de temps (T_1, ... T_n).

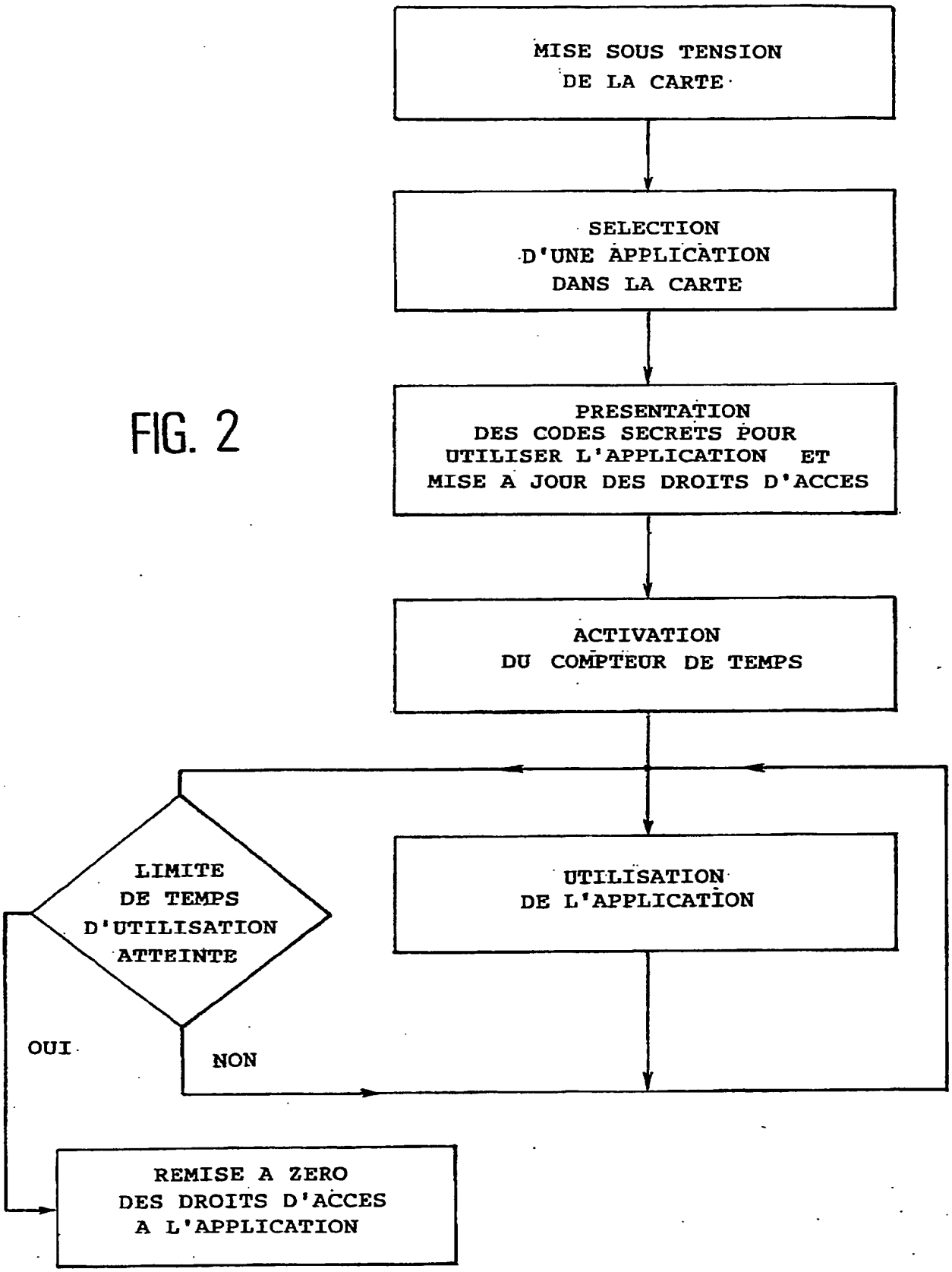
2707409

FIG. 1



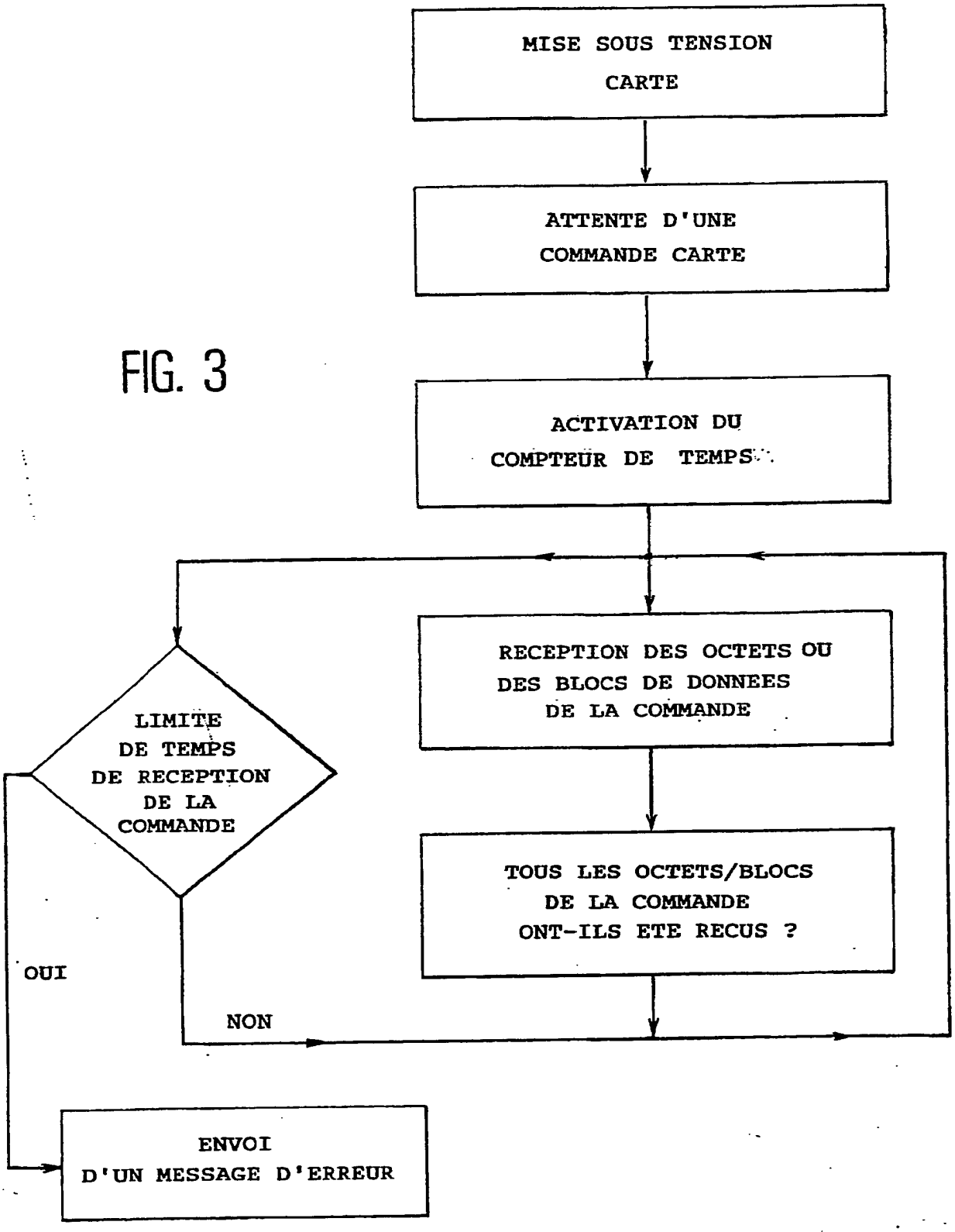
2707409

FIG. 2



2707409

FIG. 3



REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2707409
N° d'enregistrement national

FA 488428
FR 9308506

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
Y	US-A-3 633 167 (HEDIN,R.A,) * colonne 1, ligne 57 - ligne 63 * * colonne 2, ligne 22 - ligne 28 * * revendications 2,5 * ---	1-4
Y	GB-A-2 088 605 (GAO) * le document en entier * ---	1-4
A	EP-A-0 207 320 (SIEMENS) * le document en entier * -----	1-4,6

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.5)

G07C
G06K

Date d'achèvement de la recherche	Examinateur
30 Mars 1994	Herskovic, M

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)

1